УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА
Том 153, кн. 4 Физико-математические науки *2011*

УДК 519.711.3

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СТЕГАНОГРАФИЧЕСКИХ ОБЪЕКТОВ

Е.В. Разинков

Аннотация

В статье предлагается подход к математическому моделированию стеганографических объектов. Предложена математическая модель цифрового изображения в формате JPEG. Представлен эффективный алгоритм решения задачи целочисленной минимизации сепарабельной функции, возникающей при исследовании математических моделей стеганографических объектов.

Ключевые слова: математическая модель, стеганография, стеганографическая стойкость.

Введение

Цифровая стеганография – наука о скрытой передаче информации, которая осуществляется за счет встраивания секретного сообщения в некий цифровой объект, называемый стеганографическим контейнером. В качестве контейнеров используются, в частности, цифровые изображения, аудио- и видеофайлы. Цифровой объект со встроенной в него информацией называется стего.

Задача нарушителя – установить факт наличия скрытого сообщения. Ключевой параметр стеганографической системы – стеганографическая пропускная способность – количество информации, которое может быть встроено в контейнер при условии отсутствия возможности практического обнаружения встраивания.

Математическое моделирование цифровых объектов – распространенный инструмент исследования свойств стеганографических систем. Стоит отметить, однако, отсутствие моделей, которые бы обладали каждым из следующих свойств:

- рассматривали стеганографическую стойкость в теоретико-информационном смысле;
- описывали форматы используемых на практике контейнеров;
- могли непосредственно использоваться для исследования и совершенствования существующих стеганографических систем.

Мы предлагаем метод математического моделирования стеганографических объектов, позволяющий строить модели, обладающие всеми вышеперечисленными свойствами.

С помощью предлагаемого подхода мы строим модель цифрового изображения в формате JPEG – самом распространенном формате цифровых изображений в сети Интернет, что делает его наиболее привлекательным для встраивания информации стеганографическими методами.

1. Стеганографическая стойкость

1.1. Определение стеганографической системы. Рассмотрим формальное определение стеганографической системы. Пусть k – секретный стеганографический ключ из множества K возможных ключей, M – множество возможных

встраиваемых сообщений, C – множество контейнеров. Стеганографическая система состоит из двух отображений – скрывающего преобразования Emb и извлекающего преобразования Ext:

$$\mathrm{Emb} : C \times K \times M \to C,$$

$$\mathrm{Ext} : C \times K \to M$$

таких, что $\mathrm{Ext}(\mathrm{Emb}(c, k, m), k) = m$ для произвольных $c \in C,\ k \in K,\ m \in M$. Скрывающее преобразование Emb генерирует стего s путем встраивания сообщения m в контейнер c с использованием ключа k, $s = \mathrm{Emb}(c, k, m)$.

1.2. Теоретико-информационный подход к стеганографической стойкости. Пусть P_C обозначает распределение вероятностей стеганографических контейнеров, то есть $P_C(c)$ – вероятность того, что по каналу связи будет передан контейнер c, если стеганографическая передача информации не ведется. Обозначим через P_S распределение стегообъектов со встроенной информацией, через $P_S(s)$ – вероятность того, что стего s будет получено на выходе стегокодера.

Сравнение распределений P_C и P_S производится на основе расстояния Кулльбака–Лейблера (относительной энтропии), которое определяется следующим образом [1]:

$$D\left(P_c||P_s\right) = \sum_{c \in C} P_C\left(c\right) \log \frac{P_C\left(c\right)}{P_S\left(c\right)}.$$

Относительная энтропия всегда неотрицательна и равна нулю тогда и только тогда, когда $P_C \equiv P_S$. Если $D(P_C||P_S) = 0$, то стегосистема называется абсолютно стойкой, и нарушитель не может различить стего и контейнеры. Если $D(P_C||P_S) \leq \varepsilon$, то стегосистема называется ε-стойкой. Чем меньше ε, тем более стойкой является стегосистема.

2. Подход к построению математической модели стеганографического объекта

Вычисление относительной энтропии между распределениями реальных цифровых объектов, используемых в качестве стеганографических контейнеров, невозможно в силу невозможности получения сколько-нибудь точной оценки распределений P_c и P_s. Оценка относительной энтропии между распределениями контейнеров и стего позволила бы решить задачу выбора параметров стегосистемы, обеспечивающих максимальную стойкость или пропускную способность. Мы предлагаем подход к построению математических моделей стеганографических объектов, который бы обеспечивал возможность получения оценки относительной энтропии в зависимости от параметров встраивания.

2.1. Построение содержательной модели. Построение математической модели стеганографического объекта подразумевает:

- выделение конечного набора характеристик контейнера;
- определение подхода к стеганографической стойкости;
- определение способа изменения характеристик в зависимости от параметров скрывающего преобразования;
- определение свойств скрываемой информации и стеганографического ключа;
- описание структуры стеганографического объекта в целом;
- выделение параметров скрывающего преобразования, влияние которых на стойкость системы является предметом исследования.

Вышеперечисленные шаги осуществляются на этапе построения так называемой содержательной модели стеганографического контейнера.

2.1.1. Выделение конечного набора характеристик. Определение множества стегоаналитических атак, стойкость по отношению к которым будет предметом исследования, вместе со сформулированным подходом к стойкости определяет конечный набор характеристик контейнера.

2.1.2. Подход к стеганографической стойкости. В настоящей работе мы рассматриваем стойкость стеганографической системы относительно существующих стегоаналитических методов, а не гипотетических методов, которые могли бы существовать. Таким образом, при определении стойкости стегосистемы мы можем изучать лишь те характеристики стего, которые исследуются в существующих техниках стегоанализа.

Пусть c – стеганографический контейнер, а $\mathbf{f}(c)$ – вектор характеристик объекта c, которые исследуются неким фиксированным множеством стегоаналитических методов. В рамках вышеизложенного подхода цифровые объекты c_1 и c_2, для которых выполняется равенство $\mathbf{f}(c_1) = \mathbf{f}(c_2)$, неразличимы с точки зрения стегоаналитических методов из этого множества. Тогда в качестве критерия стойкости стегосистемы можно рассматривать величину $D\left(P_{\mathbf{f}(c)}||P_{\mathbf{f}(\overline{c})}\right)$, где $P_{f(c)}$ – вероятность передачи по каналу связи цифрового объекта, имеющего вектор характеристик $\mathbf{f}(c)$ при отсутствии стеганографической передачи данных, а $P_{\mathbf{f}(\overline{c})}$ – вероятность того, что переданное по каналу связи стего будет иметь вектор характеристик $\mathbf{f}\left(\overline{c}\right)$.

2.1.3. Структура стеганографического объекта. Ключевой идеей нашего подхода к структуре стеганографического объекта, контейнера или стего, является его представление в виде непересекающихся групп элементов, модифицируемых в процессе встраивания информации. Элементы контейнера разбиваются на группы таким образом, что если два элемента имеют схожие свойства и статистику, то они помещаются в одну группу, если различные – в разные группы.

Параметры скрывающего преобразования, влияние которых на стойкость системы исследуется в данной модели – количество элементов каждой из групп, модифицируемое в процессе встраивания информации.

Таким образом, стеганографический объект c, контейнер или стего, представлен в виде набора групп коэффициентов:

$$c = \{\mathbf{c}^u\}_{u=1}^{u=g},$$

где g – количество групп.

Каждая группа $\mathbf{c}^u$ представляет собой вектор коэффициентов:

$$\mathbf{c}^u = \{c_i^u\}_{i=1}^{n_u},$$

где n_u – количество элементов в u-й группе.

3. Математическая модель цифрового изображения в формате JPEG

В случае использования в качестве стеганографического контейнера цифрового изображения в формате JPEG (Joint Photographic Experts Group) квантованные коэффициенты дискретного косинусного преобразования (DCT-коэффициенты) могут быть разделены на 64 группы в зависимости от соответствующих пространственных частот. Одна из этих групп – группа DC-коэффициентов, остальные 63 группы – группы AC-коэффициентов.

Пусть n – количество DCT-коэффициентов в изображении, g – количество групп, l – количество бит во встраиваемом сообщении, n_u – количество коэффициентов в u-й группе:

$$n = \sum_{u=1}^{g} n_u,$$

k – количество коэффициентов изображения, которые могут быть изменены, k_u – количество коэффициентов в u-й группе, которые могут быть изменены (DC-коэффициенты изображения не изменяются в скрывающем преобразовании: $k_1 = 0$), k_u – количество ненулевых AC-коэффициентов в u-й группе, $u = 2, \ldots, 64$, x_u – количество DCT-коэффициентов u-й группы, используемое для встраивания информации, p_u – вероятность изменения ненулевого AC-коэффициента u-й группы в результате встраивания информации:

$$p_u = \frac{x_u}{2k_u}.$$

Под $\delta(a = b)$, $\delta(a = b, c = d)$ будем понимать следующее:

$$\delta(a = b) = \begin{cases} 1, & \text{если } a = b, \\ 0, & \text{если } a \neq b, \end{cases} \quad \delta(a = b, c = d) = \begin{cases} 1, & \text{если } a = b, c = d, \\ 0, & \text{если } a \neq b \text{ или } c \neq d. \end{cases}$$

3.1. Алгоритмы встраивания. В качестве параметров модели выбраны алгоритмы встраивания информации F5 и nsF5. Стеганографический алгоритм F5 встраивает информацию в изображения в формате JPEG путем уменьшения абсолютного значения ненулевых AC-коэффициентов, он использует матричное встраивание. Алгоритм nsF5 – это модификация алгоритма F5, использующая коды «мокрой бумаги» в целях уменьшения вносимого встраиванием искажения гистограммы DCT-коэффициентов [2]. Алгоритм nsF5 считается наиболее стойким среди методов встраивания информации в изображения в формате JPEG, не использующих дополнительную информацию [2].

3.2. Стегоаналитические атаки. В качестве характеристик, исследуемых стегоаналитиком, был выбран набор характеристик PEV-274. PEV-274 – это набор характеристик изображений в формате JPEG, состоящий из 274 характеристик, подаваемых на вход стегоаналитическому классификатору. Эффективность использования PEV-274 в стегоаналитических атаках, основанных на методе опорных векторов с гауссовым ядром, была установлена экспериментально [3].

Набор характеристик PEV-274 состоит из:

- 165 характеристик, описывающих гистограммы DCT-коэффициентов;
- 26 характеристик, описывающих корреляцию соответствующих DCT-коэффициентов соседних блоков;
- 2 характеристик, описывающих «блочность» изображения;
- 81 характеристики, описывающих корреляцию между соседними DCT-коэффициентами одного блока вдоль четырех направлений.

Полное описание характеристик и формулы их вычисления могут быть найдены в [3].

В рамках нашего подхода к стеганографической стойкости цифровое изображение в формате JPEG представляется в виде вектора своих характеристик. Вектор характеристик JPEG-изображения в рамках нашей модели состоит из следующих характеристик:

- гистограммы DCT-коэффициентов каждой группы;

• матрицы переходных вероятностей простых цепей Маркова, описывающих корреляцию между соответствующими DCT-коэффициентами соседних блоков, для каждой группы коэффициентов;

• матрицы переходных вероятностей простых цепей Маркова, описывающих корреляцию между соседними DCT-коэффициентами внутри блоков.

Таким образом, предлагаемая модель учитывает 272 из 274 характеристик PEV-274.

3.3. Вычисление характеристик контейнера. Вектор характеристик стеганографического контейнера вычисляется на основе эмпирических данных по приведенным ниже формулам.

3.3.1. Гистограммы DCT-коэффициентов. Гистограммы DCT-коэффициентов JPEG-изображения изменяются в результате встраивания информации алгоритмами F5 и nsF5. При этом 165 из 274 характеристик PEV-274 описывают гистограммы коэффициентов [3].

Пусть $\mathbf{H}$ – вектор, состоящий из g элементов – нормированных гистограмм DCT-коэффициентов для каждой из g групп:

$$\mathbf{H} = \{\mathbf{H}^u\}_{u=1}^{u=g},$$

$\mathbf{H}^u$ – вектор, описывающий нормированную гистограмму DCT-коэффициентов u-й группы:

$$\mathbf{H}^u = \{h_i^u\}_{i=-T_1}^{i=T_1},$$

где $h_i^u = \dfrac{1}{n_u}\sum\limits_{j=1}^{n_u}\delta\left(c_j^u = i\right),\ i < T_1.$

3.3.2. Корреляция между соответствующими DCT-коэффициентами соседних блоков. Корреляция между соответствующими DCT-коэффициентами соседних блоков описывается 26 из 274 характеристик PEV-274 [3].

$\mathbf{V}$ – вектор, состоящий из 64 матриц переходных вероятностей:

$$\mathbf{V} = \{\mathbf{V}^u\}_{u=1}^{u=g},$$

$\mathbf{V}^u$ – матрица переходных вероятностей, описывающая корреляцию между DCT-коэффициентами u-й группы соседних блоков:

$$\mathbf{V}^u = \left\{v_{ij}^u\right\}_{i,j=-T_2}^{i,j=T_2},$$

$$v_{ij}^u = \frac{\sum\limits_s \delta\left(c_s^u = i, c_{s+1}^u = j\right)}{\sum\limits_s \delta\left(c_s^u = i\right)}, \quad j < T_2.$$

3.3.3. Корреляция между соседними DCT-коэффициентами внутри блоков. Корреляция между коэффициентами внутри блока описывается 81 из 274 характеристик PEV-274 [3]. Существуют эффективные стегоаналитические атаки, использующие исключительно эти характеристики [4].

Обозначим через $\mathbf{M}$ вектор, состоящий из g элементов – векторов $\mathbf{M}^u$:

$$\mathbf{M} = \{\mathbf{M}^u\}_{u=1}^{u=g}.$$

Векторы $\mathbf{M}^u$ представляют собой четверки матриц:

$$\mathbf{M}^u = \left(\mathbf{M}^{u,h}, \mathbf{M}^{u,v}, \mathbf{M}^{u,d}, \mathbf{M}^{u,m}\right),$$

где $\mathbf{M}^{u,h}$, $\mathbf{M}^{u,v}$, $\mathbf{M}^{u,d}$, $\mathbf{M}^{u,m}$ – матрицы переходных вероятностей, описывающие корреляцию между соседними DCT-коэффициентами внутри блока вдоль четырех направлений: горизонтального, вертикального, вдоль главной диагонали и вдоль побочной диагонали соответственно:

$$\mathbf{M}^{u,\lambda} = \{m_{st}^{u_\lambda}\}_{s,t=-T_3}^{s,t=T_3},$$

а λ – одно из четырех направлений,

$$m_{st}^{u_\lambda} = \frac{\sum\limits_i \delta\left(|c_i^{u_\lambda}| - \left|c_i^{u_{\lambda+1}}\right| = s, \left|c_i^{u_{\lambda+1}}\right| - \left|c_i^{u_{\lambda+2}}\right| = t\right)}{\sum\limits_i \delta\left(|c_i^{u_\lambda}| - \left|c_i^{u_{\lambda+1}}\right| = s\right)}.$$

Пусть $c \in C$ – изображение-контейнер, а $\mathbf{f}(c)$ – вектор характеристик изображения c, $\mathbf{f}(\mathbf{c}) = (\mathbf{H}(\mathbf{c}), \mathbf{V}(\mathbf{c}), \mathbf{M}(\mathbf{c}))$.

3.4. Вычисление характеристик стего. Пусть $\overline{c} \in C$ – стего, полученное в результате встраивания информации в изображение-контейнер c. Вектор характеристик JPEG-изображения $\overline{c}$:

$$\mathbf{f}\left(\overline{c}\right) = \left(\overline{\mathbf{H}}, \overline{\mathbf{V}}, \overline{\mathbf{M}}\right) = \left(\overline{\mathbf{H}}\left(\overline{c}\right), \mathbf{V}\left(\overline{c}\right), \mathbf{M}\left(\overline{c}\right)\right).$$

В этом разделе мы приводим формулы для вычисления характеристик стего.

3.4.1. Гистограммы DCT-коэффициентов. Нормированные гистограммы $\overline{\mathbf{H}}$ DCT-коэффициентов стего-изображения могут быть получены на основе гистограмм контейнера $\mathbf{H}$ и вектора $\mathbf{x}$ следующим образом:

$$\overline{h}_i^u = \frac{n_u - x_u}{n_u} h_i^u + \frac{x_u}{2n_u}\left(h_i^u + h_{i+\operatorname{sgn} i}^u\right), \quad i \neq 0, \quad -T_1 + 1 < i < T_1 - 1,$$

$$\overline{h}_0^u = h_0^u + \frac{x_u}{2n_u}\left(h_1^u + h_{-1}^u\right).$$

3.4.2. Корреляция между соответствующими DCT-коэффициентами соседних блоков. Матрицы переходных вероятностей $\overline{\mathbf{V}}$ могут быть вычислены на основе матриц переходных вероятностей $\mathbf{V}$, нормированных гистограмм $\mathbf{H}$ и $\overline{\mathbf{H}}$, и вектора $\mathbf{x}$ следующим образом:

$$\overline{v}_{ij}^u = \frac{(1-p_u)^2 v_{ij}^u h_i^u}{\overline{h}_i^u} + \frac{p_u(1-p_u)\left(v_{i+\operatorname{sgn} i,j}^u h_{i+\operatorname{sgn} i}^u + v_{i,j+\operatorname{sgn} j}^u h_i^u\right)}{\overline{h}_i^u} + \\ + \frac{p_u^2 v_{i+\operatorname{sgn} i,j+\operatorname{sgn} j}^u h_{i+\operatorname{sgn} i}^u}{\overline{h}_i^u}.$$

3.4.3. Корреляция между соседними DCT-коэффициентами внутри блока. Матрицы переходных вероятностей $\overline{\mathbf{M}}$ могут быть вычислены на основе матриц переходных вероятностей $\mathbf{M}$ и условных вероятностей $p_{u_\lambda}^{s\sigma}$ и $p_{u_{\lambda+1}}^{t\tau}$, зависящих от вектора $\mathbf{x}$:

$$\overline{m}_{st}^{u_\lambda} = \sum_{\sigma=s-1}^{\sigma=s+1} \sum_{\tau=t-1}^{\tau=t+1} m_{\sigma\tau}^{u_\lambda} p_{u_\lambda}^{s\sigma} p_{u_{\lambda+1}}^{t\tau},$$

где

$$p_{u_\lambda}^{s\sigma} = p\left(\left|\overline{c}_i^{u_\lambda}\right| - \left|\overline{c}_i^{u_{\lambda+1}}\right| = s \;\middle|\; \left|c_i^{u_\lambda}\right| - \left|c_i^{u_{\lambda+1}}\right| = \sigma \;\forall i\right),$$
$$p_{u_{\lambda+1}}^{t\tau} = p\left(\left|\overline{c}_i^{u_{\lambda+1}}\right| - \left|\overline{c}_i^{u_{\lambda+2}}\right| = t \;\middle|\; \left|c_i^{u_{\lambda+1}}\right| - \left|c_i^{u_{\lambda+2}}\right| = \tau \;\forall i\right).$$

Условные вероятности $p_{u_\lambda}^{s\sigma}$, $p_{u_{\lambda+1}}^{t\tau}$ могут быть вычислены следующим образом:

$$p\left(\left|\overline{c}_i^{u_\lambda}\right| - \left|\overline{c}_i^{u_{\lambda+1}}\right| = s+1 \;\middle|\; \left|c_i^{u_\lambda}\right| - \left|c_i^{u_{\lambda+1}}\right| = s,\ \forall i\right) =$$
$$= p\left(\overline{c}_i^{u_\lambda} = c_i^{u_\lambda}\right) \cdot p\left(\left|\overline{c}_i^{u_{\lambda+1}}\right| = \left|c_i^{u_{\lambda+1}}\right| - 1\right),$$

$$p\left(\left|\overline{c}_i^{u_\lambda}\right| - \left|\overline{c}_i^{u_{\lambda+1}}\right| = s-1 \;\middle|\; \left|c_i^{u_\lambda}\right| - \left|c_i^{u_{\lambda+1}}\right| = s,\ \forall i\right) =$$
$$= p\left(|\overline{c}_i^{u_\lambda}| = |c_i^{u_\lambda}| - 1\right) \cdot p\left(\overline{c}_i^{u_{\lambda+1}} = c_i^{u_{\lambda+1}}\right),$$

$$p\left(\left|\overline{c}_i^{u_\lambda}\right| - \left|\overline{c}_i^{u_{\lambda+1}}\right| = s \;\middle|\; \left|c_i^{u_\lambda}\right| - \left|c_i^{u_{\lambda+1}}\right| = s,\ \forall i\right) = p\left(\overline{c}_i^{u_\lambda} = c_i^{u_\lambda}\right) \cdot p\left(\overline{c}_i^{u_{\lambda+1}} = c_i^{u_{\lambda+1}}\right) +$$
$$+ p\left(|\overline{c}_i^{u_\lambda}| = |c_i^{u_\lambda}| - 1\right) \cdot p\left(\left|\overline{c}_i^{u_{\lambda+1}}\right| = \left|c_i^{u_{\lambda+1}}\right| - 1\right),$$

где $p\left(\overline{c}_i^u = c_i^u\right) = 1 - \dfrac{k_u}{n_u} p_u$, $p\left(|\overline{c}_i^u| = |c_i^u| - 1\right) = \dfrac{k_u}{n_u} p_u$.

3.5. Постановка задачи вычисления оптимальных параметров скрывающего преобразования. Задача вычисления оптимального количества информации для встраивания в каждую из g групп коэффициентов (вектора $\mathbf{x}$) является задачей целочисленной минимизации функции относительной энтропии между распределениями векторов характеристик контейнеров и стего.

Задача минимизации функции относительной энтропии для модели изображения в формате JPEG формулируется следующим образом:

$$D\left(P_{\mathbf{f}(c)} || P_{\mathbf{f}(\overline{c})}\right) \to \min,$$
$$\sum_{u=1}^{g} x_u = l, \quad 0 \le x_u \le k_u, \quad u = 1, 2, \ldots, g,$$

где

$$D\left(P_{\mathbf{f}(c)} || P_{\mathbf{f}(\overline{c})}\right) = \sum_{u=1}^{g} n_u \left(\sum_{i,j=-T_2}^{T_2} v_{ij}^u h_i^u \log_2 \frac{v_{ij}^u}{\overline{v}_{ij}^u} + \sum_{\lambda} \sum_{s,t=-T_3}^{T_3} m_{st}^{u_\lambda} \psi_s^{u_\lambda} \log_2 \frac{m_{st}^{u_\lambda}}{\overline{m}_{st}^{u_\lambda}} \right),$$
$$\psi_s^{u_\lambda} = p\left(|c^{u_\lambda = u}| - |c^{u_{\lambda+1}}| = s\right).$$

4. Быстрые алгоритмы целочисленной минимизации сепарабельных функций

Для построенных с помощью предлагаемого метода математических моделей стеганографических объектов характерна сепарабельная функция относительной энтропии в силу подхода к структуре стеганографического объекта. Задача вычисления оптимальных параметров скрывающего преобразования будет сводиться, в свою очередь, к задаче целочисленной минимизации сепарабельной функции. Заметим, что функция относительной энтропии в модели изображения в формате JPEG не является сепарабельной.

Пусть D – сепарабельная функция:

$$D(\mathbf{x}) = \sum_{i=1}^{g} d_i(x_i),$$

где $\mathbf{x} = \{x_i\}_{i=1}^{i=g}$, $0 \le x_i \le n_i$, $x_i \in \mathbf{Z}$, $i = 1, 2, \ldots, g$.

4.1. Случай выпуклых неубывающих функций d_i. Задача целочисленной минимизации имеет вид:

$$D(\mathbf{x}) = \sum_{i=1}^{g} d_i(x_i) \to \min,$$
$$\Delta d_i(x_i) \geq 0, \quad \Delta d_i(x_i) - \Delta d_i(x_i - 1) > 0, \tag{1}$$
$$0 \leq x_i \leq n, \quad x_i \in \mathbf{Z}, i = 1, 2, \ldots, g, \quad \sum_{i=1}^{g} x_i = l,$$

где $\Delta d_i(x_i) = d_i(x_i) - d_i(x_i - 1)$.

Эффективные алгоритмы целочисленной минимизации выпуклой функции существуют и известны. Опишем общеизвестный «жадный» алгоритм минимизации применительно к сформулированной выше задаче.

«Жадный» алгоритм минимизации:

Шаг 1. Полагаем $\overline{l} := 0$; $x_i := 0$; $\Delta\overline{d}_i := \Delta d_i(0)$, $i = 1, 2, \ldots, g$;

Шаг 2. Вычисляем $j = \arg\min\limits_{i, x_i < n} \Delta\overline{d}_i$; $\overline{l} := \overline{l} + 1$; $x_j := x_j + 1$; $\Delta\overline{d}_j := \Delta d_j(x_j)$;

Шаг 3. Если $\overline{l} < l$, перейти к Шагу 2;

Шаг 4. Результат: вектор $\mathbf{x} = \{x_i\}_{i=1}^{g}$.

Теорема 1. *Пусть* $\mathbf{x}$ *– решение задачи* (1). *Имеет место* $\overline{\mathbf{x}}$ *– решение задачи* (1), $\sum\limits_{i=1}^{g} \overline{x}_i = \overline{l}$, $\overline{l} > l$, *то справедливы неравенства*

$$\overline{x}_i \geq x_i, \quad i = 1, 2, \ldots, g.$$

Доказательство. Доказательство проведем от противного. Пусть утверждение теоремы неверно, то есть существует непустое множество индексов

$$I = \{i_1, i_2, \ldots, i_{\overline{g}}\}$$

такое, что $\overline{x}_i < x_i$, если $i \in I$; $\overline{x}_i \geq x_i$, если $i \notin I$.

Покажем теперь, что существует вектор $\widetilde{\mathbf{x}} = \{\widetilde{x}_i\}_{i=1}^{g}$ такой, что $\sum\limits_{i=1}^{g} \widetilde{x}_i = \overline{l}$, $D(\widetilde{\mathbf{x}}) < D(\overline{\mathbf{x}})$, $0 \leq \widetilde{x}_i \leq n$, $i = 1, 2, \ldots, g$.

Построим вектор $\widetilde{\mathbf{x}} = \{\widetilde{x}_i\}_{i=1}^{i=g}$ следующим образом:

$$\widetilde{x}_i = x_i + a_i, \quad i = 1, 2, \ldots, g,$$

где $\mathbf{a} = \{a_i\}_{i=1}^{i=g}$ – произвольный вектор, состоящий из целочисленных элементов, удовлетворяющих следующим условиям:

$$a_i = 0, \quad \text{если} \quad i \in I,$$

$$0 \leq a_i \leq \overline{x}_i - x_i, \quad \text{если} \quad i \notin I,$$

$$\sum_{i=1}^{g} a_i = \overline{l} - l.$$

Так как $\sum\limits_{i \notin I} (\overline{x}_i - x_i) > \overline{l} - l$, то вектор $\widetilde{\mathbf{x}}$, удовлетворяющий этим условиям, существует. Заметим также, что существует $j \notin I$ такое, что $a_j > 0$.

Имеем, что $\sum\limits_{i=1}^{g} \widetilde{x}_i = \overline{l}$, поскольку $\sum\limits_{i=1}^{g} \widetilde{x}_i = \sum\limits_{i=1}^{g} x_i + \sum\limits_{i=1}^{g} a_i = l + \overline{l} - l = \overline{l}$.

Теперь покажем, что $D(\widetilde{\mathbf{x}}) < D(\overline{\mathbf{x}})$. Рассмотрим разность:

$$\sum_{i=1}^{g} d_i(\overline{x}_i) - \sum_{i=1}^{g} d_i(\widetilde{x}_i) = \sum_{i \in I} (d_i(\overline{x}_i) - d_i(\widetilde{x}_i)) + \sum_{i \notin I} (d_i(\overline{x}_i) - d_i(\widetilde{x}_i)). \tag{2}$$

В силу того, что $\Delta d_i(x_i) \geq 0$, $\Delta d_i(x_i) - \Delta d_i(x_i - 1) > 0$, $0 \leq x_i \leq n$, $i = 1, 2, \ldots, g$, мы можем записать для целых y и z, $0 \leq z < y \leq n$ и натурального s, $s \leq z$:

$$d_i(y) - d_i(z) > d_i(y - s) - d_i(z - s).$$

Так как $\widetilde{x}_i - x_i \geq 0$, если $i \notin I$, и $\exists j \notin I : \widetilde{x}_j - x_j > 0$, то справедливо неравенство

$$\sum_{i \notin I} (d_i(\overline{x}_i) - d_i(\widetilde{x}_i)) > \sum_{i \notin I} (d_i(\overline{x}_i - (\widetilde{x}_i - x_i)) - d_i(\widetilde{x}_i - (\widetilde{x}_i - x_i))). \tag{3}$$

Построим вектор $\widehat{\mathbf{x}} = \{\widehat{x}_i\}_{i=1}^{g}$:

$$\widehat{x}_i = \begin{cases} \overline{x}_i, & i \in I \\ \overline{x}_i - a_i, & i \notin I. \end{cases}$$

Заметим, что $\sum\limits_{i=1}^{g} \widehat{x}_i = \sum\limits_{i=1}^{g} \overline{x}_i - \sum\limits_{i=1}^{g} a_i = \overline{l} - \overline{l} + l = l$.

Рассмотрим правую часть неравенства (3):

$$\sum_{i \in I} (d_i(\overline{x}_i) - d_i(\widetilde{x}_i)) + \sum_{i \notin I} (d_i(\overline{x}_i - (\widetilde{x}_i - x_i)) - d_i(\widetilde{x}_i - (\widetilde{x}_i - x_i))) =$$
$$= \sum_{i \in I} (d_i(\widehat{x}_i) - d_i(x_i)) + \sum_{i \notin I} (d_i(\widehat{x}_i) - d_i(x_i)) = D(\widehat{\mathbf{x}}) - D(\mathbf{x}).$$

Имеем, что $D(\widehat{\mathbf{x}}) \geq D(\mathbf{x})$, так как $\mathbf{x}$ – решение задачи (1) и $\sum\limits_{i=1}^{g} \widehat{x}_i = l$. Отсюда и из (2), (3) следует:

$$D(\overline{\mathbf{x}}) - D(\widetilde{\mathbf{x}}) > 0,$$

что приводит к противоречию, так как $\overline{\mathbf{x}}$ – решение задачи (1). Теорема доказана. □

Следствие 1. *Решение задачи* (1) *может быть найдено с помощью «жадного» алгоритма.*

Следствие 2. *Если* $\overline{\mathbf{x}}$ *– решение задачи* (1) *и* $\Delta d_i(x_i) \geq 0$, $\Delta d_i(x_i) - \Delta d_i(x_i - 1) \geq 0$, $0 \leq x_i \leq \overline{x}_i$, *для любого* i, *то вектор* $\overline{\mathbf{x}}$ *может быть найден с помощью «жадного» алгоритма.*

4.2. Случай невыпуклых возрастающих функций d_i. Рассматривается задача

$$\begin{aligned} & D(\mathbf{x}) \to \min, \\ & 0 \leq x_i \leq n, \quad x_i \in \mathbf{Z}, \quad \forall i, \\ & \sum_{i=1}^{g} x_i = l, \end{aligned} \tag{4}$$

где функции d_i удовлетворяют следующим условиям:

1. $\Delta d_i(x_i) \geq 0$;

2. $\forall i\ \exists z_i,\ 0 < z_i < n$:

$\Delta d_i(x_i) - \Delta d_i(x_i - 1) \geq 0$ при $x_i \leq z_i$,

$\Delta d_i(x_i) - \Delta d_i(x_i - 1) < 0$ при $n > x_i > z_i$;

3. $\forall i, j$: если $\exists x,\ 0 < x < n$: $\Delta d_i(x) < \Delta d_j(x)$, то $\Delta d_i(x) < \Delta d_j(x)$ для любого $x,\ 0 < x \leq n$.

4.3. Эффективный алгоритм решения задачи минимизации сепарабельной функции. В рамках настоящей работы мы предлагаем эффективный алгоритм нахождения решения задачи (4). Прежде чем перейти к описанию самого алгоритма, введем некоторые обозначения.

Не ограничивая общности, будем считать, что $\forall i, j,\ i < j\ :\ \exists x,\ \Delta d_i(x) < \Delta d_j(x)$.

Рассмотрим задачу минимизации

$$\begin{aligned} &\sum_{i=u}^{g} d_i\left(y_i^{u,l}\right) \to \min, \\ &y_i^{u,l} = 0, \quad \forall i < u, \\ &0 \leq y_i^{u,l} \leq n, \quad y_i^{u,l} \in \mathbf{Z}, \quad \forall i \geq u, \\ &\sum_{i=u}^{g} y_i^{u,l} = l. \end{aligned} \tag{5}$$

Через $\mathbf{y}^{u,l} = \left\{y_i^{u,l}\right\}_{i=1}^{i=g}$ обозначим вектор, получаемый в результате применения «жадного» алгоритма для решения задачи (5).

Введем функции $f_u(l) = \sum\limits_{i=u}^{g} d_i\left(y_i^{u,l}\right)$, $\Delta f_u(l) = f_u(l) - f_u(l-1)$, и $D_{u,l}(x_u) = \sum\limits_{i=1}^{u-1} d_i(n) + d_u(x_u) + f_{u+1}(l - x_u - n(u-1))$, положим

$$\Delta D_{u,l}(x_u) = D_{u,l}(x_u) - D_{u,l}(x_u - 1) = \Delta d_u(x_u) - \Delta f_{u+1}(l - x_u + 1 - n(u-1)).$$

Введем также вектор $\mathbf{q} = \{q_i\}_{i=1}^{i=g}$, $q_i = y_i^{i,l-n(i-1)}$.

Алгоритм решения задачи (4) состоит в следующем:

Шаг 1. Полагаем $k = \left\lfloor \dfrac{l}{n} \right\rfloor$;

Шаг 2. Если $y_1^{1,l} < z_1$, то полагаем $s := 1$, иначе $s := \max\limits_{q_u \geq z_u} u$;

Шаг 3. Для каждого $u = s, s+1, \ldots, k$ вычисляем $D_u := \min\limits_{q_u \leq x_u \leq n} D_{u,l}(x_u)$, $\alpha_u := \arg\min\limits_{q_u \leq x_u \leq n} D_{u,l}(x_u)$;

Шаг 4. Выбираем v такое, что $D_v = \min\limits_{s \leq u \leq t} D_u$;

Шаг 5. Результат: вектор $\overline{\mathbf{x}} = \{\overline{x}_i\}_{i=1}^{i=g}$:

$$\overline{x}_i = \begin{cases} n, & i < v, \\ \alpha_v, & i = v, \\ y_i^{v+1,l-n(v-1)-\alpha_v}, & i > v. \end{cases} \tag{6}$$

Лемма 1. *Пусть* $\mathbf{x}$ *– решение задачи* (4) *или вектор, полученный в результате применения «жадного» алгоритма. Тогда не существует* $i,\ j,\ i \neq j$ *таких, что* $z_i \leq x_i < n,\ z_j \leq x_j < n$.

Доказательство. Докажем от противного. Пусть $\mathbf{x}$ – решение задачи (4) или вектор, полученный в результате применения «жадного» алгоритма, и

$$\exists i, j,\ i \neq j:\ z_i \leq x_i < n,\ z_j \leq x_j < n,$$

то есть $\Delta d_i(x_i) > \Delta d_i(x_i + 1)$ и $\Delta d_j(x_j) > \Delta d_j(x_j + 1)$.

Не ограничивая общности, будем считать, что $\Delta d_i(x_i) \leq \Delta d_j(x_j)$. Тогда $\Delta d_i(x_i + 1) < \Delta d_j(x_j)$, откуда следует, что $d_i(x_i + 1) + d_j(x_j - 1) < d_i(x_i) + d_j(x_j)$. Если $\mathbf{x}$ – решение задачи (4), то мы получили противоречие.

Теперь покажем, что вектор $\mathbf{x}$ не может быть получен применением «жадного» алгоритма. Пусть на Шаге 2 некоторой итерации алгоритма i-й элемент промежуточного вектора равен x_i, а j-й – $x_j - 1$. Но $\Delta d_i(x_i + 1) < \Delta d_j(x_j)$, поэтому на Шаге 2 следующей итерации снова будет выбран i-й элемент, который примет значение $x_i + 1$. Это означает, что $\mathbf{x}$ не может быть получен применением «жадного» алгоритма. Лемма доказана. □

Лемма 2. *Пусть* $\overline{\mathbf{x}}$ *– решение задачи* (4)*, или вектор, полученный в результате применения «жадного» алгоритма, и существует такое* x*, что* $\Delta d_i(x) < \Delta d_j(x)$*. Тогда* $\overline{x}_i \geq \overline{x}_j$.

Доказательство. Докажем от противного: пусть $\overline{x}_i < \overline{x}_j$. Покажем, что $d_i(\overline{x}_j) + d_j(\overline{x}_i) < d_i(\overline{x}_i) + d_j(\overline{x}_j)$.

По условию леммы существует $x,\ 0 < x < n$: $\Delta d_i(x) < \Delta d_j(x)$, откуда в силу свойств функций d_i следует справедливость неравенства $\Delta d_i(x) < \Delta d_j(x)$ для любого $x,\ 0 < x < n$, поэтому

$$d_i(\overline{x}_j) - d_i(\overline{x}_i) < d_j(\overline{x}_j) - d_j(\overline{x}_i),$$

следовательно, $d_i(\overline{x}_j) + d_j(\overline{x}_i) < d_i(\overline{x}_i) + d_j(\overline{x}_j)$. Это означает, что $\overline{\mathbf{x}}$ не может являться решением задачи (4), мы получили противоречие.

Теперь покажем, что вектор $\overline{\mathbf{x}}$ не мог быть получен в результате применения «жадного» алгоритма.

В силу свойств функций d_i справедливо следующее утверждение:

$$\max_{x \leq x_i} \Delta d_i(x) < \max_{x \leq x_i} \Delta d_j(x).$$

Заметим также, что $\Delta d_i(x_i + 1) < \Delta d_j(x_i + 1)$, то есть j-й элемент не мог быть увеличен до того, как i-й примет значение $x_i + 1$. Лемма доказана. □

Лемма 3. *Пусть* $\overline{\mathbf{x}}$ *– решение задачи* (4)*, а* $\mathbf{x}$ *– вектор, полученный в результате применения жадного алгоритма для решения задачи* (4)*. Тогда не существует* i *такого, что*

$$x_i > \max(\overline{x}_i, z_i).$$

Доказательство. Переформулируем утверждение леммы следующим образом: если $x_i > z_i$, то $\overline{x}_i \geq x_i$. Докажем от противного. Пусть утверждение леммы неверно и существует i: $x_i > z_i$, $\overline{x}_i < x_i$. Пусть $t = x_i - \overline{x}_i$.

Возможны два случая: $x_i = n$ и $x_i < n$.

Пусть $x_i = n$. По лемме 1 разность

$$\sum_{k \neq i} d_k(\overline{x}_k) - \sum_{k \neq i} d_k(x_k)$$

минимальна, если существует j, для которого $x_j > z_j$, $x_j \le \overline{x}_i$, и $overline x_j = x_j + t$. Покажем, что

$$d_i(x_i) - d_i(\overline{x}_i) < d_j(x_j + t) - d_j(x_j).$$

По лемме 2 $\Delta d_i(x) < \Delta d_j(x)$ для любого x, $0 \le x \le n$, и $x_j > z_j$, $x_j \le \overline{x}_i$, поэтому

$$\Delta d_i(\overline{x}_i + k) < \Delta d_j(\overline{x}_i + k) < \Delta d_j(x_j + k), \quad \forall k\ 0 \le k \le t.$$

Мы получили, что

$$\sum_k d_k(\overline{x}_k) > \sum_k d_k(x_k),$$

а это приводит к противоречию, так как $\overline{\mathbf{x}}$ – решение задачи (4) по условию леммы. Для случая $x_i = n$ лемма доказана.

Рассмотрим случай $x_i < n$. По лемме 1 $x_j < z_j$, $j \ne i:\ x_j \ne n$. Так как $\overline{x}_i > z_i$, $\overline{x}_j < z_j$, то для любого $j \ne i:\ x_j \ne n$.

Вектор $\mathbf{x}$ получен в результате применения «жадного» алгоритма, поэтому

$$\Delta d_i(z_i) < \Delta d_j(x_j) \quad \forall j \ne i:\ x_j \ne n.$$

$x_j \le \overline{x}_j < z_j$, $\forall j \ne i:\ x_j \ne n$ и $\overline{x}_i > z_i$, откуда следует, что для $j \ne i:\ x_j \ne n$:

$$\Delta d_i(x) < \Delta d_i(z_i) < \Delta d_j(\widetilde{x}_j) \quad \forall x,\ \forall \widetilde{x}_j : \overline{x}_i \le x \le x_i, \quad x_j \le \widetilde{x}_j \le \overline{x}_j$$

Как и в предыдущем случае, получаем

$$\sum_k d_k(\overline{x}_k) > \sum_k d_k(x_k),$$

что приводит к противоречию, так как $\overline{\mathbf{x}}$ – решение задачи (4) по условию леммы.

Лемма доказана. □

Теорема 2. *Вектор* $\overline{\mathbf{x}} = \{\overline{x}_i\}_{i=1}^{i=g}$, *определенный согласно* (6), *является решением задачи* (4).

Доказательство. В силу лемм 1 и 2 существует j такое, что $\overline{x}_i = n$, $i = 1, 2, \ldots, j$; $\overline{x}_i < z_i$, $i = j, j+1, \ldots, g$; $\overline{x}_{j+1} \le \overline{x}_j \le n$.

По следствию 2 к теореме 1, если j и $\overline{x}_j$ найдены верно, то остальные элементы вектора $\overline{\mathbf{x}}$ могут быть найдены с помощью «жадного» алгоритма.

Алгоритм перебирает все значения j от k, определяемого в Шаге 1, до s, определяемого в Шаге 2, $k \ge s$.

Покажем, что $s \le j \le k$. Очевидно, что $k \ge j$. Покажем, что $j \ge s$.

Для случая $s = 1$ доказательство очевидно. Для случая $s > 1$ приведем доказательство от противного. Пусть $s > 1$ и $j < s$, $n \ge q_s \ge z_s$. По лемме 3 получаем, что $n \ge \overline{x}_s \ge z_s$. Но j было выбрано таким, что $\overline{x}_i < z_i$, $i > j$. Мы получили противоречие.

Так как алгоритм для каждого j, $s \le j \le k$, перебирает все значения $\overline{x}_j$, среди которых может присутствовать оптимальное для данного j, то среди значений D_u, вычисленных на Шаге 3, обязательно присутствует минимальное, а соответствующий ему вектор $\overline{\mathbf{x}}$, как следует из изложенного выше, является решением задачи (4). Теорема доказана. □

Заключение

В настоящей работе мы представили метод математического моделирования стеганографических объектов, позволяющий оценивать стеганографическую стойкость в теоретико-информационном смысле. Этот подход может быть применен для построения моделей реальных стеганографических объектов различных форматов. Предложена математическая модель цифрового изображения в формате JPEG и поставлена задача вычисления оптимальных параметров скрывающего преобразования. Предложен эффективный алгоритм целочисленной минимизации сепарабельной функции определенного вида, доказана оптимальность решения, получаемого с помощью этого алгоритма.

Summary

E.V. Razinkov. Mathematical Models of Steganographic Objects.

In this paper, we propose an approach to mathematical modeling of steganographic objects and a mathematical model of JPEG image. We also provide a fast algorithm for integer minimization of separable functions.

Key words: mathematical model, steganography, steganographic security.

Литература

1. *Cachin C.* An Information-Theoretic Model for Steganography // Information Hiding, 2nd Int. Workshop. Lecture Notes in Computer Science, V. 1525. – 1998. – С. 306–318.
2. *Fridrich J., Pevny T., Kodovsky J.* Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities // Proc. of the 9th ACM Multimedia and Security Workshop. – 2007. – С. 3–14.
3. *Pevny T., Fridrich J.* Merging Markov and DCT Features for Multi-Class JPEG Steganalysis // Proc. SPIE Electronic Imaging, Photonics West. – 2007. – С. 03–04.
4. *Shi Y.Q., Chen C., Chen W.* A Markov process based approach to effective attacking JPEG steganography // Proc. of the 8th Information Hiding Workshop. – 2006. – С. 249–264.

Поступила в редакцию
19.09.11

Разинков Евгений Викторович – ассистент кафедры системного анализа и информационных технологий Казанского (Приволжского) федерального университета.

E-mail: *razinkov@steganography.ru*